WHAT IS CLAIMED IS:

1. A method for controlling access to network resources, the method comprising:

receiving at a network node, a request to assume the identity of the network node;

detecting whether the request originates with a user having a permissible virtual identity characteristic; and

if the user has a permissible virtual identity characteristic, sharing the identity of the network node with the user, wherein network resources permit access to resources by the user as if it had the network node identity.

2. A method for providing authorized access to a network resource, the method comprising:

receiving, at a preauthorized machine, from a first user a request to access a network resource;

detecting whether said first user is authorized to access said network resource; and

if said step of detecting indicates that said first user is authorized, assigning the first user the identity of the preauthorized machine.

3. The method of claim 2 further comprising:

receiving, at said preauthorized machine, from a second user a request to access a network resource detecting whether said second user is authorized to access said network resource; and

if said step of detecting indicates that said second user is authorized, assigning the second user the identity of the preauthorized machine.

4. The method of claim 3 wherein said first and second users are assigned the identity of the preauthorized machine during overlapping time periods.

5. The method of claim 2 wherein said step of detecting includes,

receiving an identifier associated with the first user;

comparing the received identifier to a table of authorized identifiers; and

determining whether the received identifier matches any of the authorized identifiers based on the results of the comparing operation.

a2
cont

6. The method of claim 2 wherein said step of detecting includes,

receiving a first identifier associated with the first user and a second identifier associated with a requested resource;

comparing the received first identifier/second identifier pair to contents of an authorized memory; and

determining that the user is authorized to access the requested resource if a match is found for the first and second identifier pair in the memory during the comparing step.

7. A method for providing access control with respect to assets available on a web server, the method comprising:

providing a plurality of machines authorized to access the web server;

associating with each authorized machine an access table storing authorization information;

coupling one of the authorized machines to an access requester;

verifying that said requester is authorized to access an asset on the web server with reference to said access table associated with the authorized machine to which the requester is coupled; and

allowing the requester to assume the identity of said authorized machine to which the register is coupled after verifying that said requester is authorized.

8. The method of claim 7 wherein said plurality of authorized machines includes a first authorized machine that is authorized to access a first subset of assets at the web server and a second authorized machine that is authorized to access a second subset of assets at the web server, wherein said second subset differs from said first subset.

a2 cont

~~9. The method of claim 7 wherein said plurality of authorized machines includes a first authorized machine that is authorized to access a first subset of assets at the web server and a second authorized machine that is authorized to access a second subset of assets at the web server, wherein said second subset overlaps with said first subset.~~

~~10. The method of claim 9 wherein said first and second subsets are identical.~~